What's New in Internet Security & Acceleration (ISA) Server 2004

Avinash Lotke
Technology Specialist
Microsoft Corporation
avinashl@microsoft.com

Microsoft TechNet

Security Issues Today

- 14B devices on the Internet by 2010 [1]
- 35M remote users by 2005 [2]
- 65% increase in dynamic Web sites [3]
- From 2000 to 2002 reported incidents rose from 21,756 to 82,094 [4]
- Nearly 80 percent of 445 respondents surveyed said the Internet has been a frequent point of attack, up from 57 percent just four years ago [5]

- 90% detected security breaches [6]
- 85% detected computer viruses [6]
- 95% of all breaches avoidable with an alternative configuration [7]
- Approximately 70 percent of all Web attacks occur at the application layer [8]

1 Source: Forrester Research
2 Source: Information Week, 26 November 2001
3 Source: Netcraft summary
4 Source: CERT, 2003
5 Source: CSI/FBI Computer Crime and Security Survey
6 Source: Computer Security Institute (CSI) Computer Crime and Security Survey 2002
7 Source: CERT, 2002
8 Source: Gartner Group

Customer Impact

Application Layer Attacks

- Identity Theft
- Web Site Defacement
- Unauthorized Access
- Modification of Data, Logs and Records
- Theft of Proprietary Information
- Service Disruption

Implications

Compliance:

- Basel 2 (EU)
- Data Protection Act (EU)
- Sarbanes Oxley
- Gramm Leach Blilely
- US Patriot Act
- HIPAA
- The Privacy Act (CA)

Litigation

- File Sharing
- Piracy
- HR Issues
- Shareholder Suits

Traditional Firewalls

Wide open to advanced attacks	■ Code Red, Nimda ■ SSL-based attacks
Hard to manage	■ Security is complex ■ IT already overloaded
Performance vs. security tradeoff	■ Bandwidth too expensive ■ Too many moving parts
Limited capacity for growth	■ Not easily upgradeable ■ Don’t scale with business

Perimeter Security Evolution

Wide open to advanced attacks	Application-level protection
Hard to manage	Easier to use
Performance vs. security tradeoff	Security and performance
Limited capacity for growth	Extensibility and scalability

Introducing: ISA Server 2004

The advanced application layer firewall, VPN and Web cache solution that enables customers to maximize IT investments by improving network security & performance

Advanced protection

Application layer security designed to protect Microsoft applications

Ease of use

Efficiently deploy, manage, and enable new usage scenarios

Fast, secure access

Empowers you to connect users to relevant information on your network in a cost efficient manner

TechNet

You need to…

ISA Delivers:

You need to…	ISA Delivers:
Securely make e-mail available to outside employees	Exchange publishing
Securely make internal applications available on the Internet	Web and Server Publishing
Enable partners to access relevant information on my network	Integrated S2S VPN and FW
Secure and flexible remote access, while protecting my corporate network	Integrated RRAS VPN and FW
Securely connect my branch offices to the corporate office	Integrated FW, VPN, Cache
Control Internet Access and protect my clients from malicious Internet	FW, Web Proxy
Ensure fast access to the most frequently used web content	Caching

ISA Server 2004 New Features

Updated security architecture

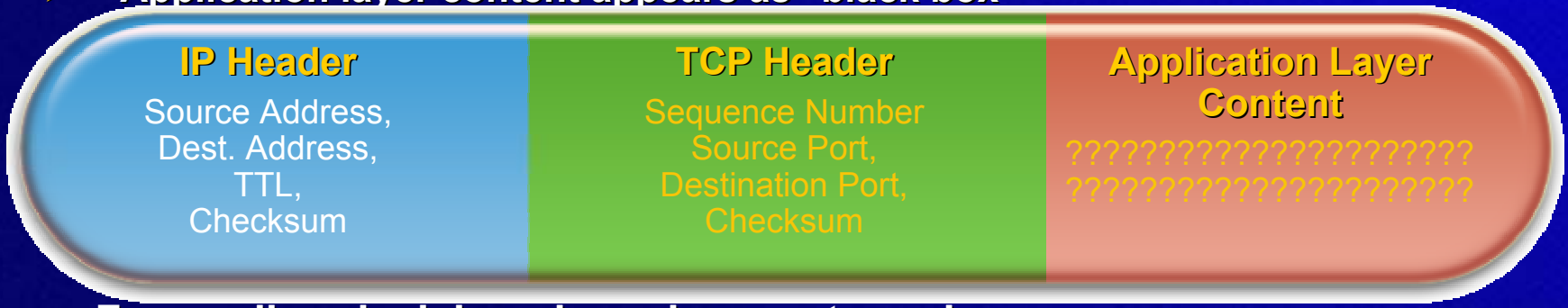
Advanced protection

Application layer security designed to protect Microsoft applications

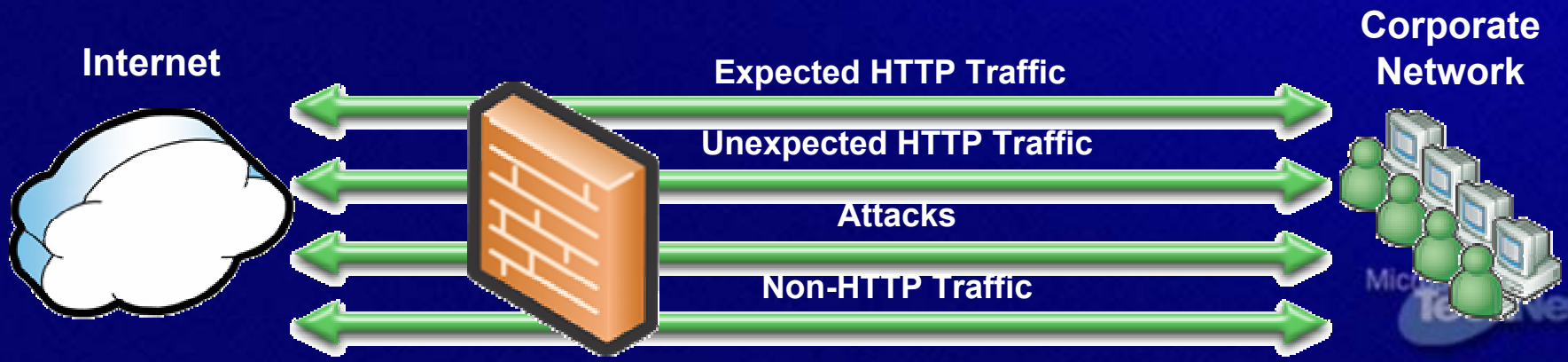
Deep content inspection	• Enhanced HTTP, customizable prtcl. filters • Comprehensive/flexible policies • Stateful routing for all IP traffic
Enhanced Exchange Server Integration	• Support for Outlook RPC over HTTP • Enhanced Outlook Web Access security • Easy to use configuration wizards
Fully integrated VPN	• Unified firewall-VPN filtering • Built-in support for site-to-site IPsec TM • Integrates with Windows Quarantine
Secure IIS and SPPS	• SSL Bridging for IIS and SPS • Easy to use Web publishing wizards • AD, RADIUS, SecurID authentication

A Traditional Firewall's View Of A Packet

- Only packet headers are inspected
  - Application layer content appears as "black box"

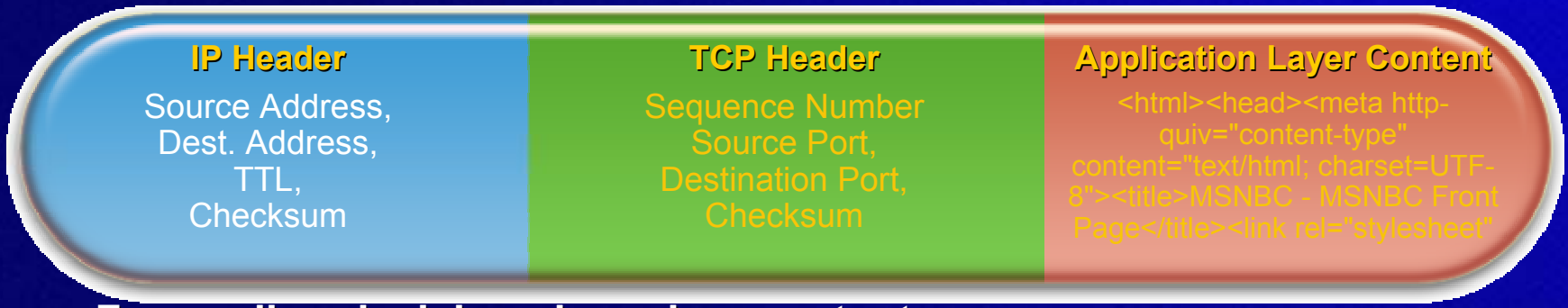


- Forwarding decisions based on port numbers
  - Legitimate traffic and application layer attacks use identical ports

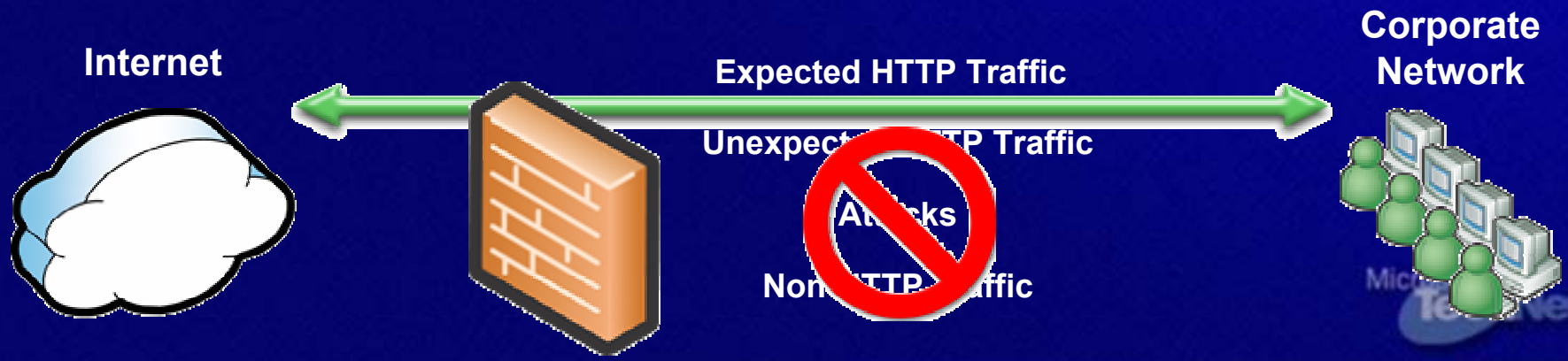


ISA Server's View Of A Packet

- Packet headers and application content are inspected



- Forwarding decisions based on content
  - Only legitimate and allowed traffic is processed



ISA Server 2004 New Features

New management tools and user interface

Ease of Use

Efficiently deploy, manage, and enable new usage scenarios

Multi-network architecture	• Unlimited network definitions and types • Firewall policy applied to all traffic • Per network routing relationships
Network templates and wizards	• Wizard automates nwk routing relationships • Supports 5 common network topologies • Easily customized for sophisticated scenarios
Visual policy editor	• Unified firewall/VPN policy w/one rule-base • Drag/drop editing w/scenario-driven wizards • XML-based configuration import-export
Enhanced trouble-shooting	• All new monitoring dashboard • Real-time log viewer • Content sensitive task panes

ISA Server 2004 New Features

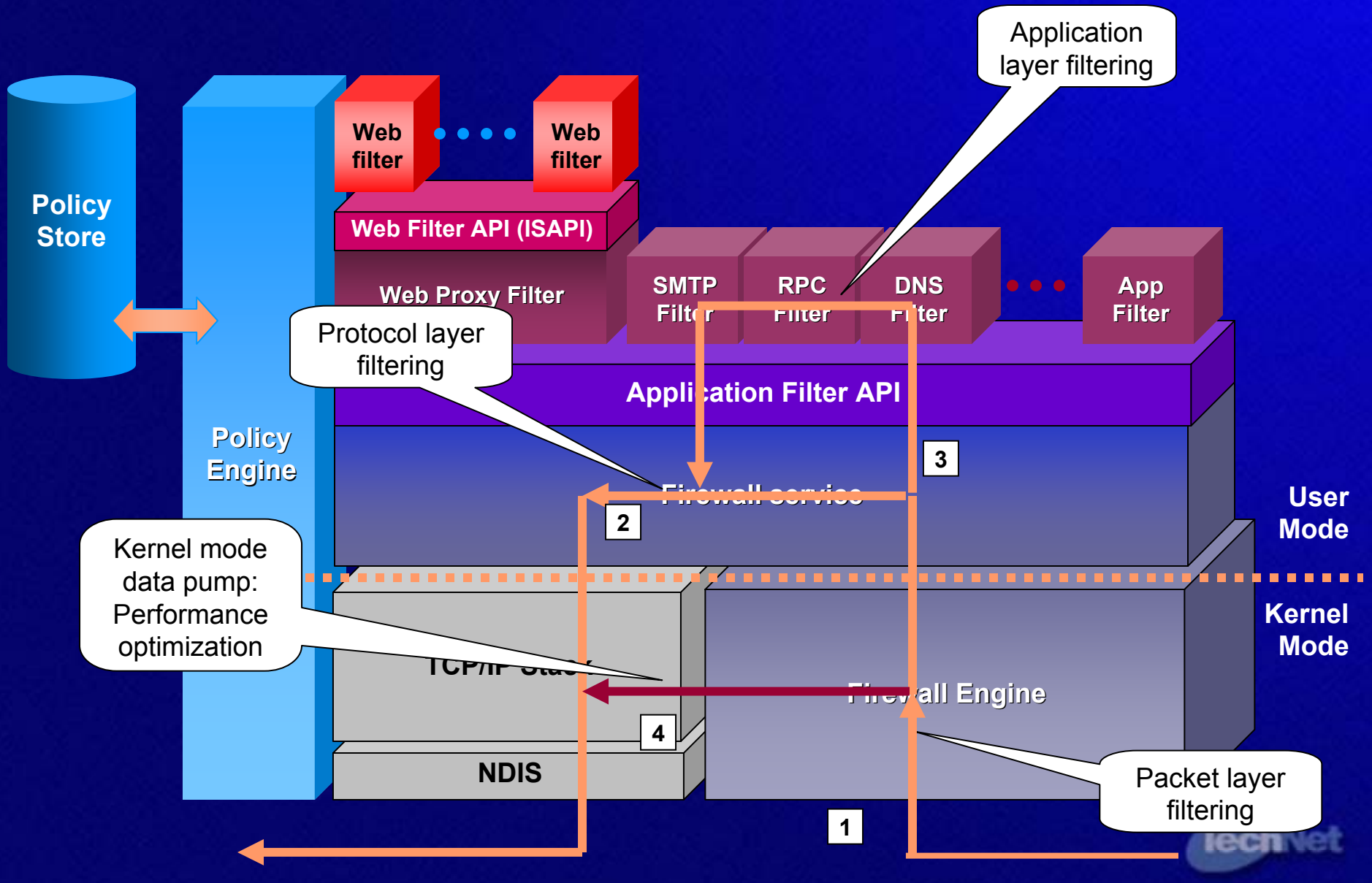
Continued commitment to integration

Fast, secure access

Empowers you to connect users to relevant info. on your network

Enhanced architecture	• High speed data transport • Utilizes latest Windows and PC hardware • SSL bridging unloads downstream servers
Web cache	• Updated policy rules • Serve content locally • Pre-fetch content during low activity periods
Internet access control	• User- and group-based Web usage policy • Extensible by third parties
Comprehensive authentication	• New support for RADIUS and RSA SecurID • User- & group-based access policy • Third party extensibility

ISA 2004 Architecture



Enterprise Edition

- Differences for EE over SE
  - Increased scalability and availability
  - Distributed Management: large-scale deployments with array and enterprise policies
- Key Features
  - Bi-directional NLB support for firewall arrays
  - Enterprise policy distribution and management
  - Enterprise array monitoring console
  - AD/AM-based policy store
  - CARP and hierarchical caching
  - Unlimited SMP
  - MOM pack / integration
  - Automatic array configuration / wizards
  - Array-level logging / alerting

Microsoft TechNet

Subject to change

OS Compatibility and Migration

- ISA 2004 SE
  - Microsoft Windows® 2000 Server or Advanced Server with Service Pack 4 or later, Windows 2000 Datacenter Server
  - Windows Server 2003 Standard Edition or Enterprise Edition Recommend
- ISA 2004 EE
  - Windows Server 2003 Standard Edition or Enterprise Edition only

Microsoft TechNet

ISA Server 2004 Top Partners

- Antivirus
  - McAfee and GFI
- URL Filtering
  - SurfControl and Websense
- Application Filtering
  - Forum Systems and Akonix
- Authentication/ID
  - RSA
- Reporting
  - WebSpy and NetIQ
- Load Balancing / HA
  - Rainfinity
- SSL Acceleration
  - AEP
- SSL VPN
  - Everywhere Networks
- Deployment
  - Various Microsoft Partners

Microsoft TechNet

Demo

Microsoft TechNet

Celestix
MSA Series Appliance

Lee Wei Shun
Product Manager
Celestix Networks Pte Ltd

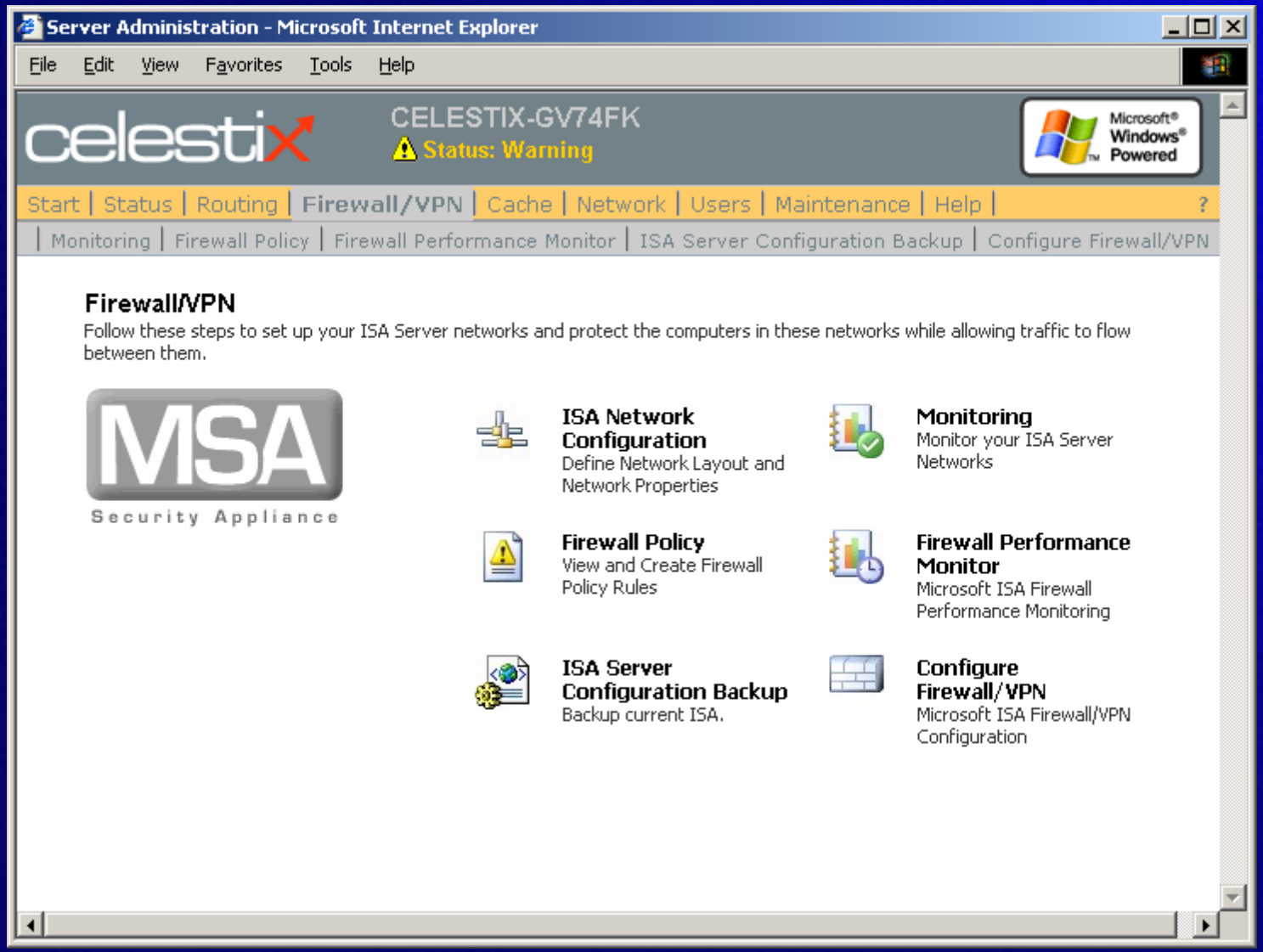
Microsoft TechNet

Product Features

celestix Firewall, VPN and Caching Appliance

- True APPLIANTIZED version of ISA 2004
- Optimized appliance form factor
- Web GUI for remote management
- LCD front panel for easy network configuration and status display
- One button system recovery to factory default
- Installs in less than 30 minutes
- Powered by Embedded Windows Server 2003
- Available in 3 models

MSA Web UI


Server Administration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
celestix
CELESTIX-GV74FK
Status: Warning
Microsoft® Windows® Powered
Start | Status | Routing | Firewall/VPN | Cache | Network | Users | Maintenance | Help | ?
Monitoring | Firewall Policy | Firewall Performance Monitor | ISA Server Configuration Backup | Configure Firewall/VPN
Firewall/VPN
Follow these steps to set up your ISA Server networks and protect the computers in these networks while allowing traffic to flow between them.
MSA
Security Appliance
ISA Network Configuration
Define Network Layout and Network Properties
Monitoring
Monitor your ISA Server Networks
Firewall Policy
View and Create Firewall Policy Rules
Firewall Performance Monitor
Microsoft ISA Firewall Performance Monitoring
ISA Server Configuration Backup
Backup current ISA.
Configure Firewall/VPN
Microsoft ISA Firewall/VPN Configuration

Microsoft TechNet

Market Segments Addressed

Small Business

- 1-100 users
- One or two sites
- No security staff
- DSL connection

Mid-sized Business

- 101-500 users
- Multiple sites
- May or may not have dedicated security staff
- T1 or T3 connection

Enterprise

- 500+ users
- Dedicated staff
- Large number of sites
- T3 or OC-3 connection

MSA2000

MSA4000

MSA5000

Microsoft TechNet

Contacts

- **Asia Pacific**

+65 6-844-1301

sales@celestix.com

- **North America**

510-668-0700

sales@us.celestix.com

For more information, please visit www.celestix.com

Microsoft TechNet

Session Summary

- ISA Server 2004 provides many benefits
  - Advanced application layer firewall
  - VPN
  - Web cache solution
- ISA Server 2004 offers many improvements over ISA Server 2000
  - Enhanced user interface
  - New features
  - Improved functionality

Microsoft TechNet

Key takeaways

- Downloadable 120-day eval at www.microsoft.com/isaserver
- Product availability / pricing
  - August 2004
  - Per-processor license, $1499 ERP (USD)
- Best protection for Microsoft applications
- Helps protect against the growing number of application layer-based security threats

Microsoft TechNet

Microsoft®

Your potential. Our passion.™

© 2004 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.

Microsoft TechNet

Additional Ref.

Microsoft TechNet

Application Layer Filtering

- Modern threats call for deep inspection
  - Protects network assets from exploits at the application layer: Nimda, Slammer...
  - Provides the ability to define a fine grain, application level, security policy
  - Best protection for Microsoft applications
- Application filtering framework
  - Built in filters for common protocols
    - HTTP, SMTP, RPC, FTP, H.323, DNS, POP3, Streaming media
  - Scenario-driven design
  - Extensible plug-in architecture

Microsoft TechNet

VPN Protection

- Detunneled traffic is inspected
  - Injected back to the stack
  - ISA Server sees traffic on stack hooks
- VPN traffic is segregated
  - VPN network: all addresses allocated to VPN users
  - IP addresses dynamically added/removed
  - VPN network available in ISA Server admin
- IPSec Tunnel Mode support
  - Provides connectivity to branch office VPN
  - Simplified tools for administration
- Quarantine support
  - Quarantined users placed in quarantine network
  - IP addresses dynamically added/removed
  - Quarantine network available in ISA Server admin

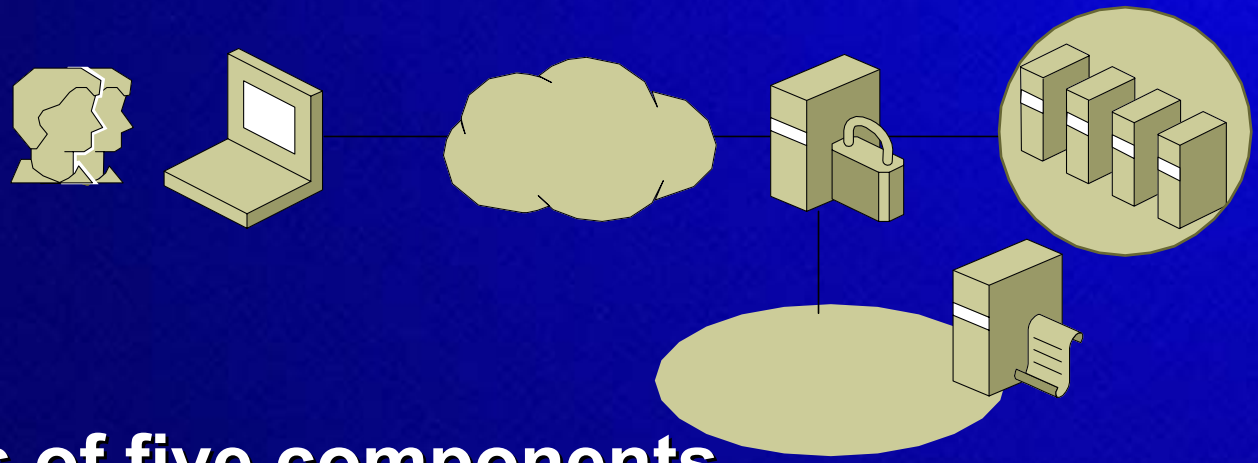
Microsoft TechNet

VPN Quarantine

- VPN Quarantine ensures the security and configuration of clients connected via remote user VPN
- Compliments Patch Management Strategy
  - Helps “buy time” for patch management
  - Enables patch management outside of Windows administrative boundaries

Microsoft TechNet

Customer example: VPN Quarantine



- Consists of five components
  - Quarantine Policy Service – Server
  - Quarantine Release Service – Server
  - QuarantineClient.EXE – Client
  - ISA Configuration
    - ISA Server 2004 – Firewall Rules + Enforcement
    - RRAS – Integrated with ISA

Microsoft TechNet

Engine Security Enhancements

- Flood-DoS protection
  - SYN-flood protection
  - Client connection quota
    - Applicable to Worm/Virus floods
  - Spoofed UDP packet flooding mitigation
- Attack/Intrusion Detection
  - IP options, DNS Attacks, IP half-scan, Port scan
- IP options filtering
  - Filter out individual options
- Lockdown mode
  - Restrict firewall machine access on service failures

Microsoft TechNet

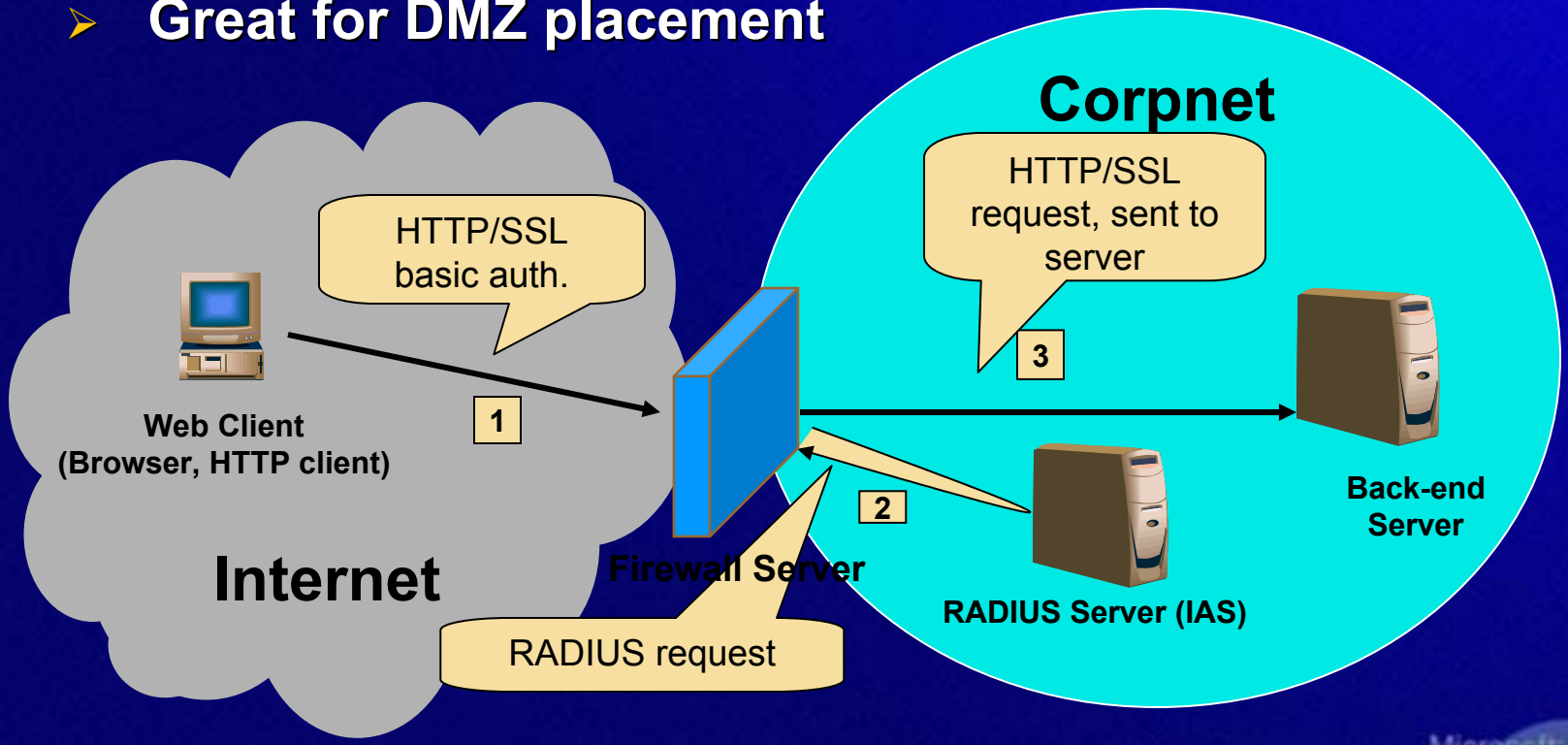
Authentication Framework

- Multi source authentication
  - Firewall client authentication
    - Transparent user authentication
      - LSP is loaded in user context
      - Application transparent, Protocol independent
    - Kerberos/NTLM
  - Web proxy authentication
    - Proxy auth, Reverse proxy auth, Pass through auth
    - SSL bridging
    - Basic, digest, NTLM, Kerberos, Certificates
    - RADIUS authentication, SecurID authentication
    - CRL support
    - Extensible!
  - VPN clients
    - EAP (certificates, smartcards, others)
    - MS-CHAPv2, CHAP, (S-PAP, PAP)
    - RADIUS / Windows
- Extensible authentication/authorization framework
  - Third party filters can register their own auth namespaces

TechNet

RADIUS Authentication

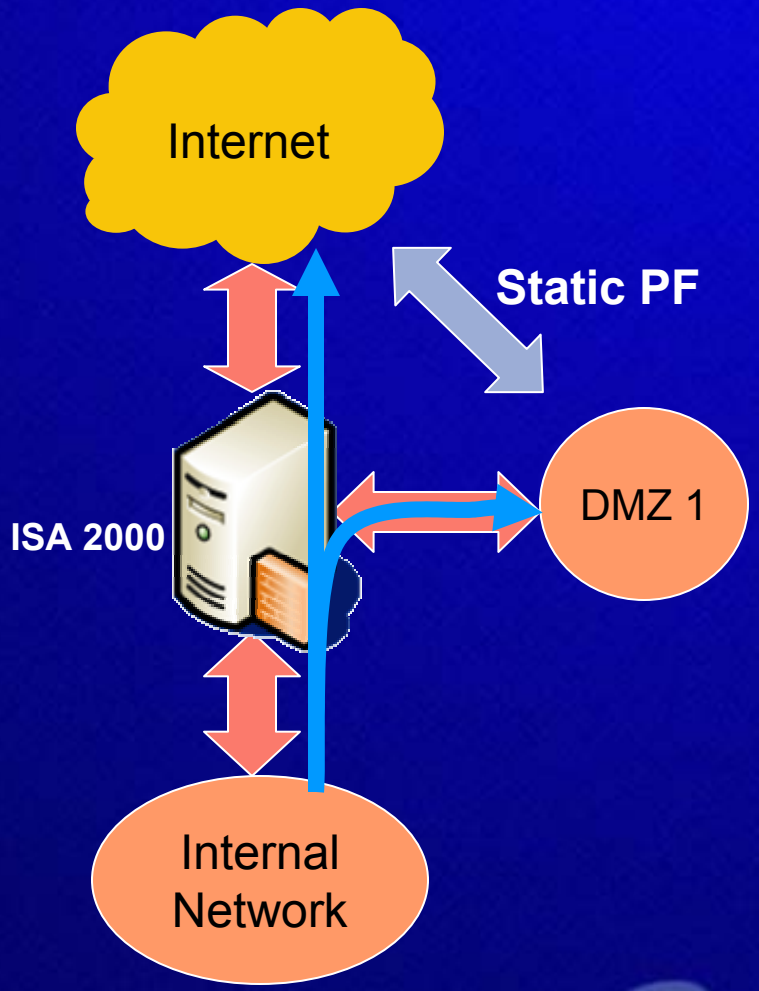
- Federation through RADIUS proxies
- Can be used for centralized authentication services
- Domain membership not required
  - Great for DMZ placement



Microsoft TechNet

ISA 2000 (old) Networking Model

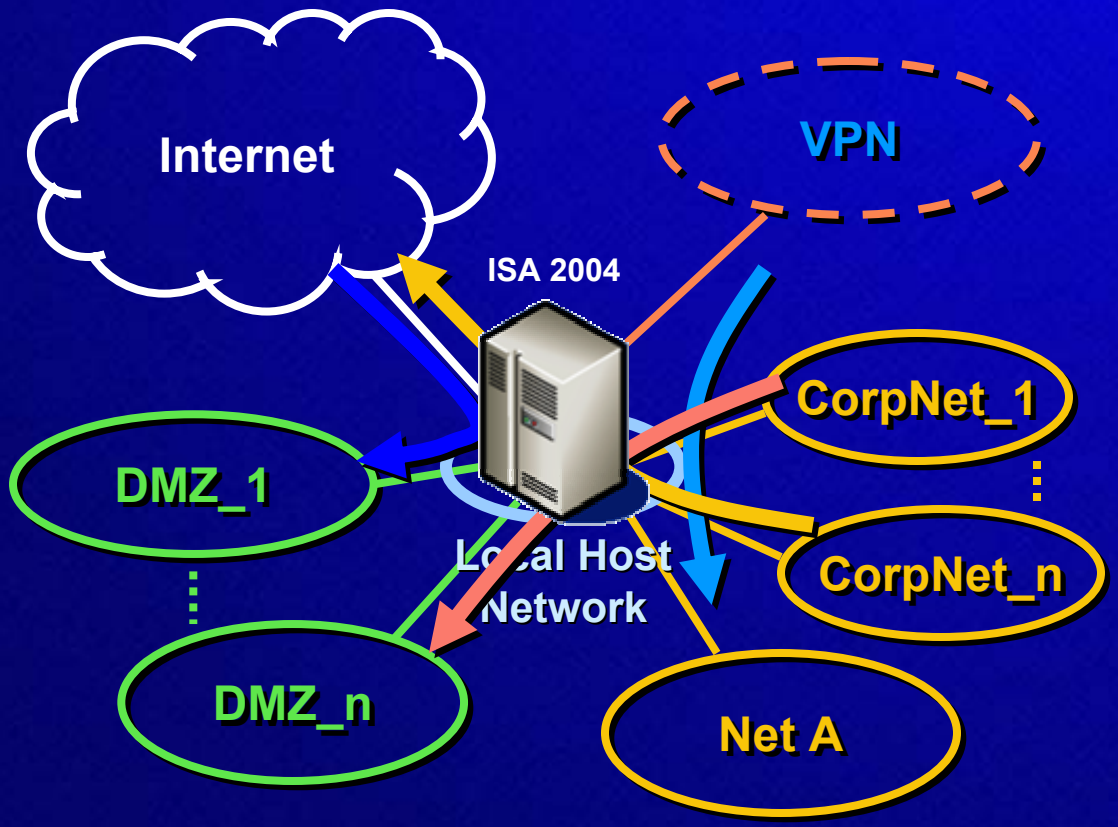
- Fixed zones
  - "IN" = LAT
  - "OUT" = DMZ, Internet
- Packet filter only on external interfaces
- Single outbound policy
  - NAT always
- Static filtering from DMZ to Internet



Microsoft TechNet

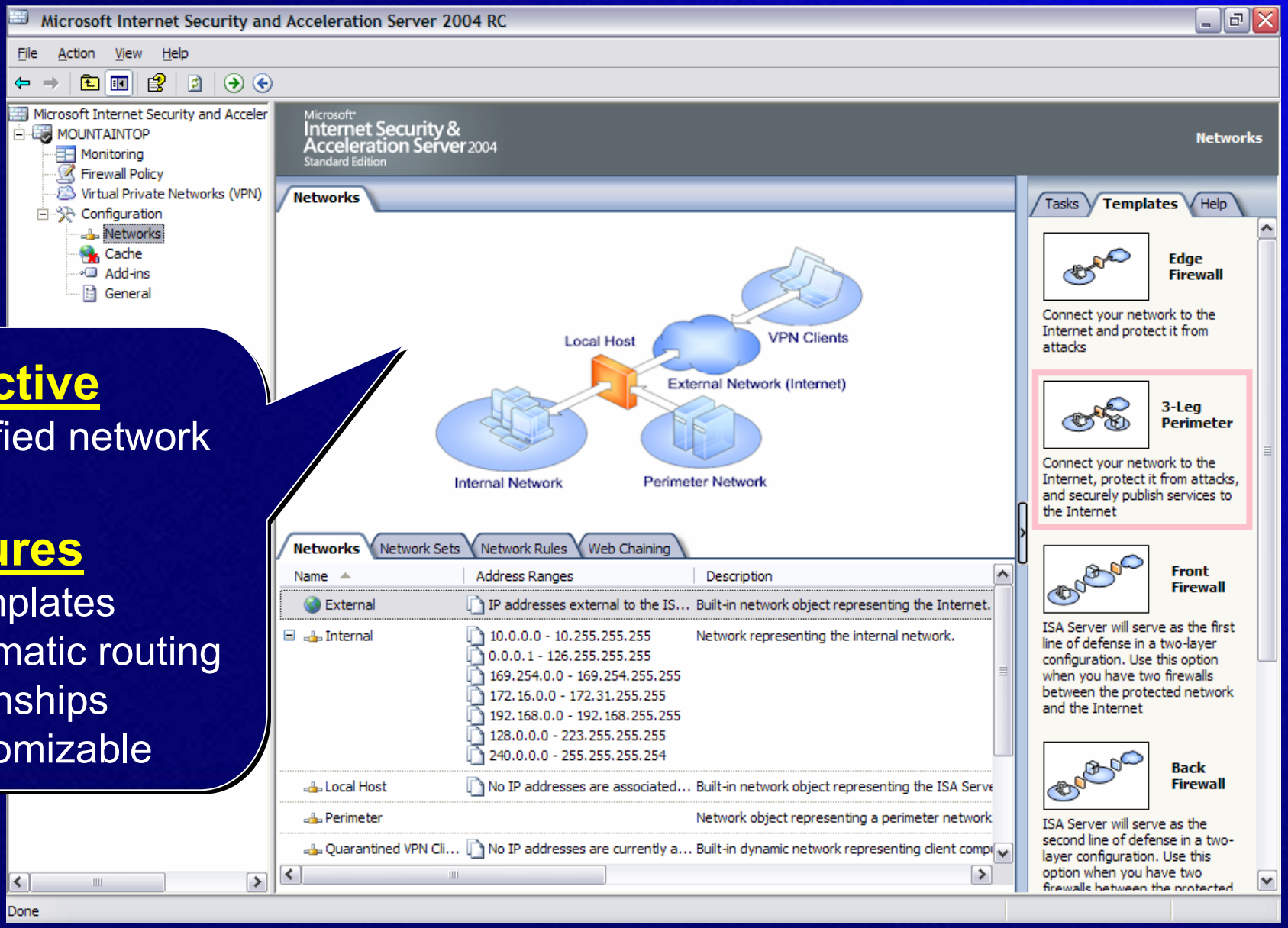
ISA 2004 Networking Model

- Any number of networks
- VPN as network
- Localhost as network
- Assigned relationships (NAT/Route)
- Per-Network policy
- Packet filtering on all interfaces
- Support for PnP & DoD
- *Any topology, any policy*



Microsoft TechNet

Network Templates



Objective

Simplified network config

Features

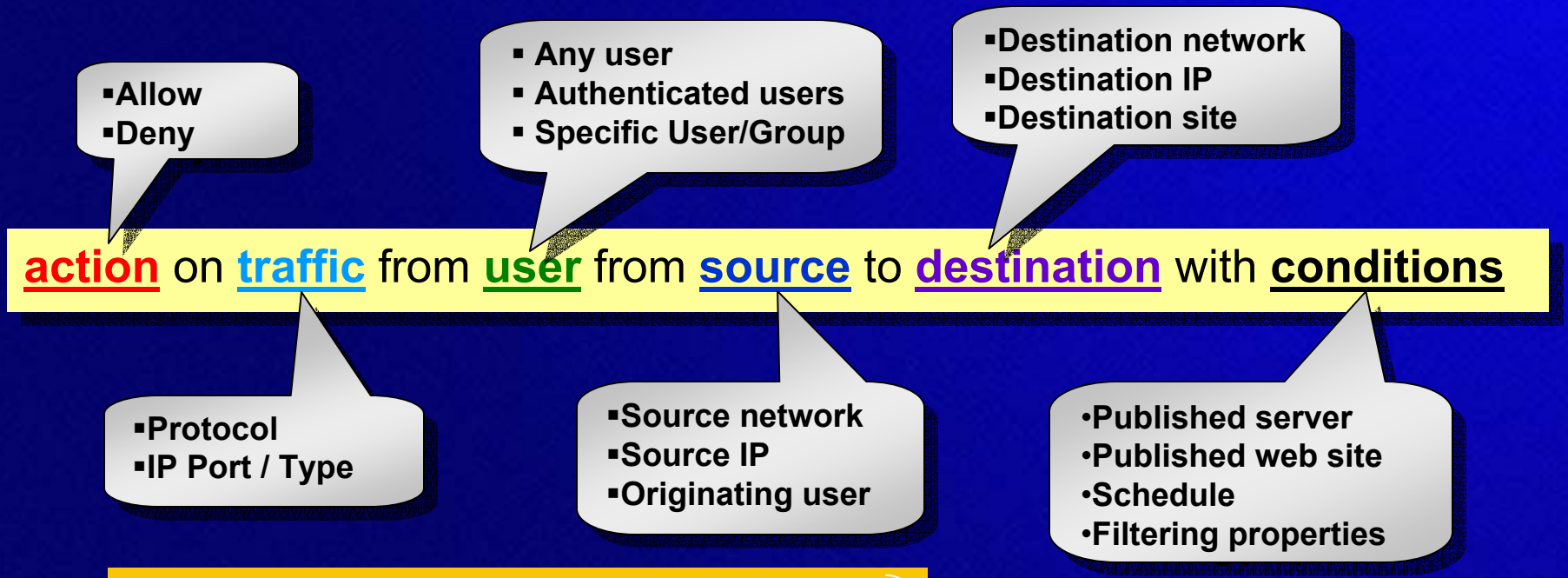
- 5 templates
- Automatic routing relationships
- Customizable

ISA 2004 Policy Model

- Single, ordered rule base
  - More logical and easier to understand
  - Easier to view and to audit
- New unified rule structure
  - Applicable to all types of policy
  - Three master types of rule “templates”
    - Access rules
    - Server Publishing rules
    - Web Publishing rules
  - Application filtering properties a part of the rule
- Default System Policy

Microsoft TechNet

Rule Structure & Policy Mapping



Basic ISA 2004 rules:

- Protocol rules
- Site and Content rules
- Static packet filters
- Publishing rules
- Web publishing rules
- Selected filtering configuration

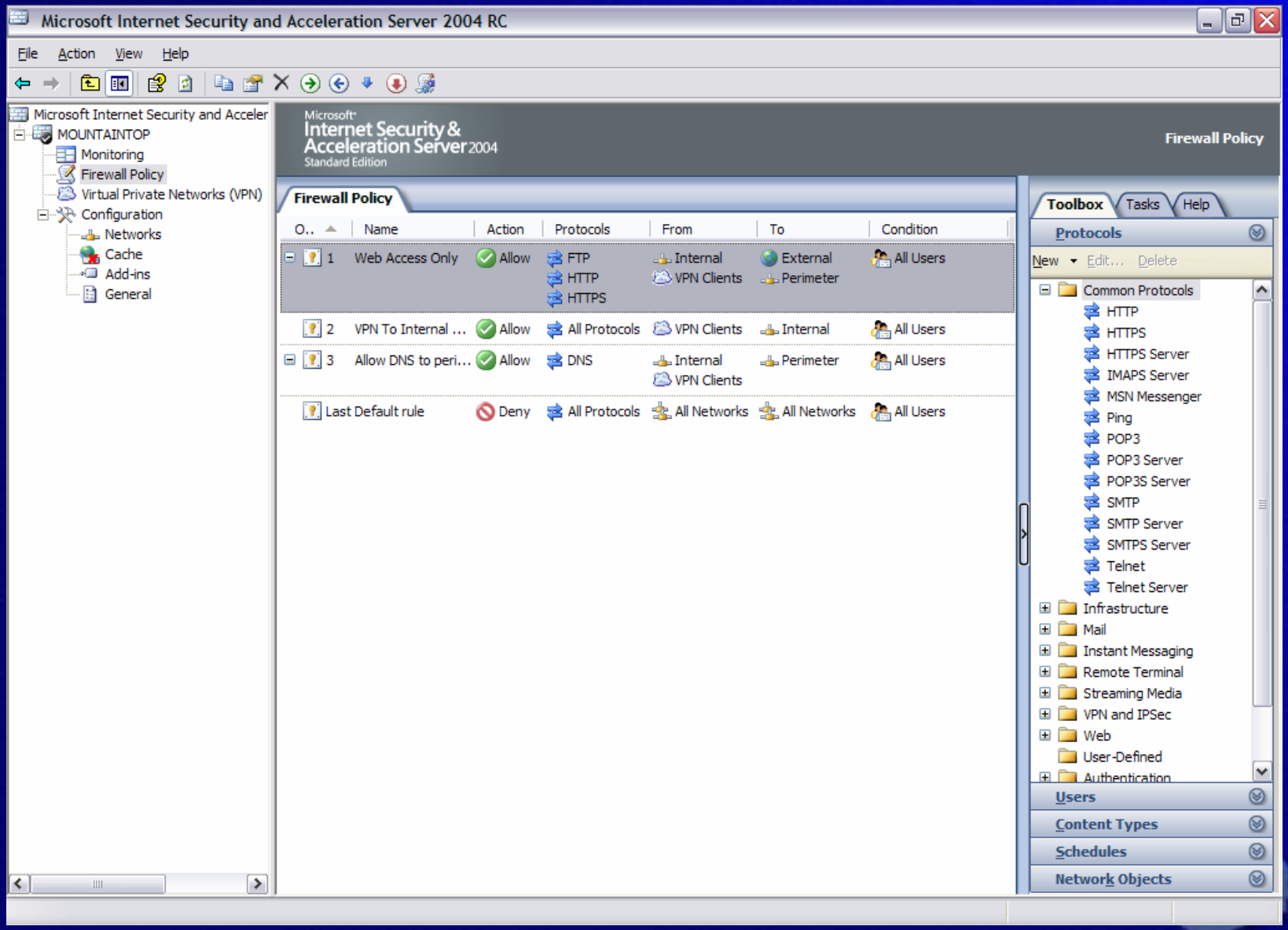
Firewall policy

Other ISA 2004 rules:

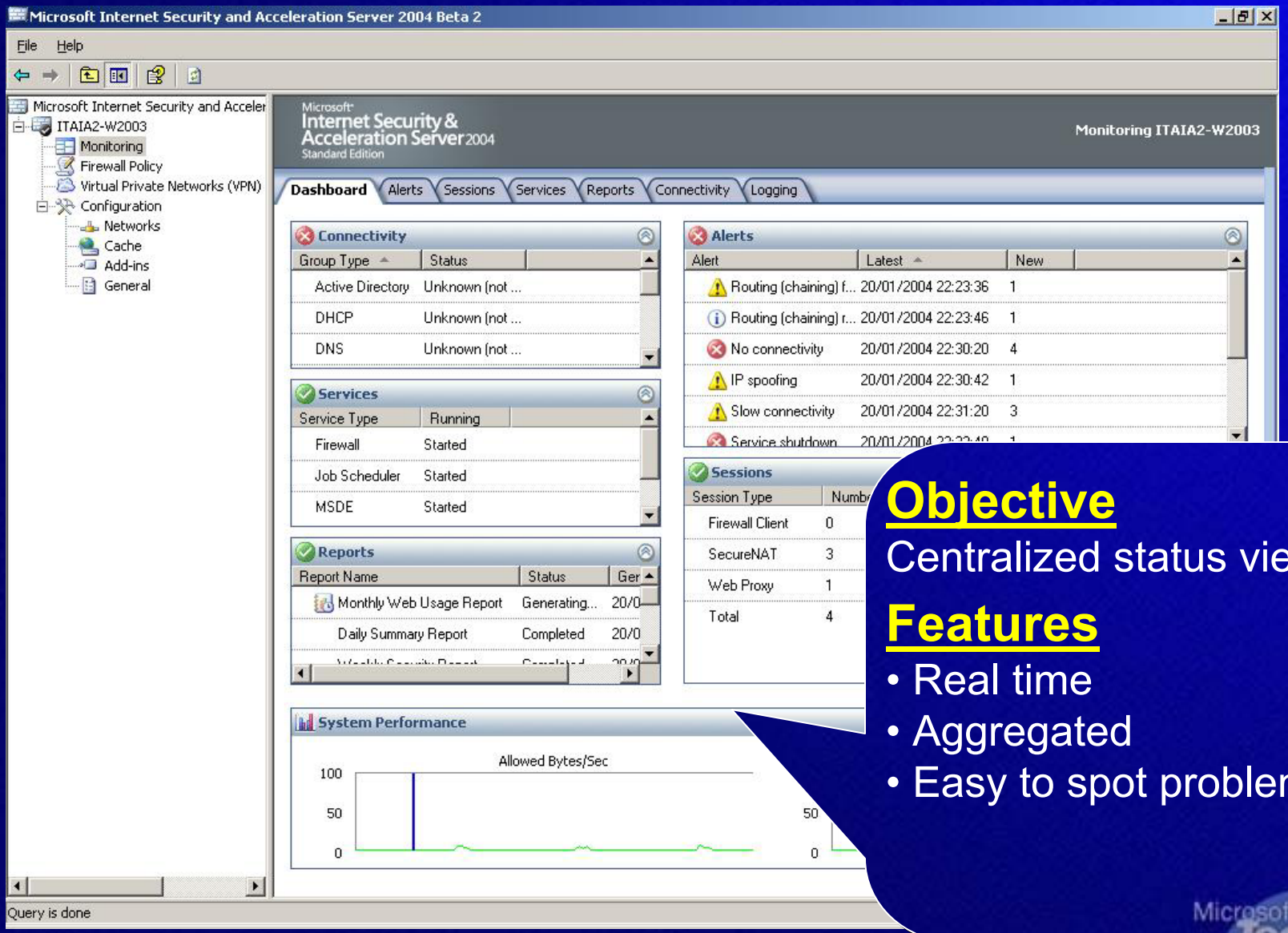
- Address translation rules
- Web routing rules

Configuration policy

Visual Policy Editor



Dashboard



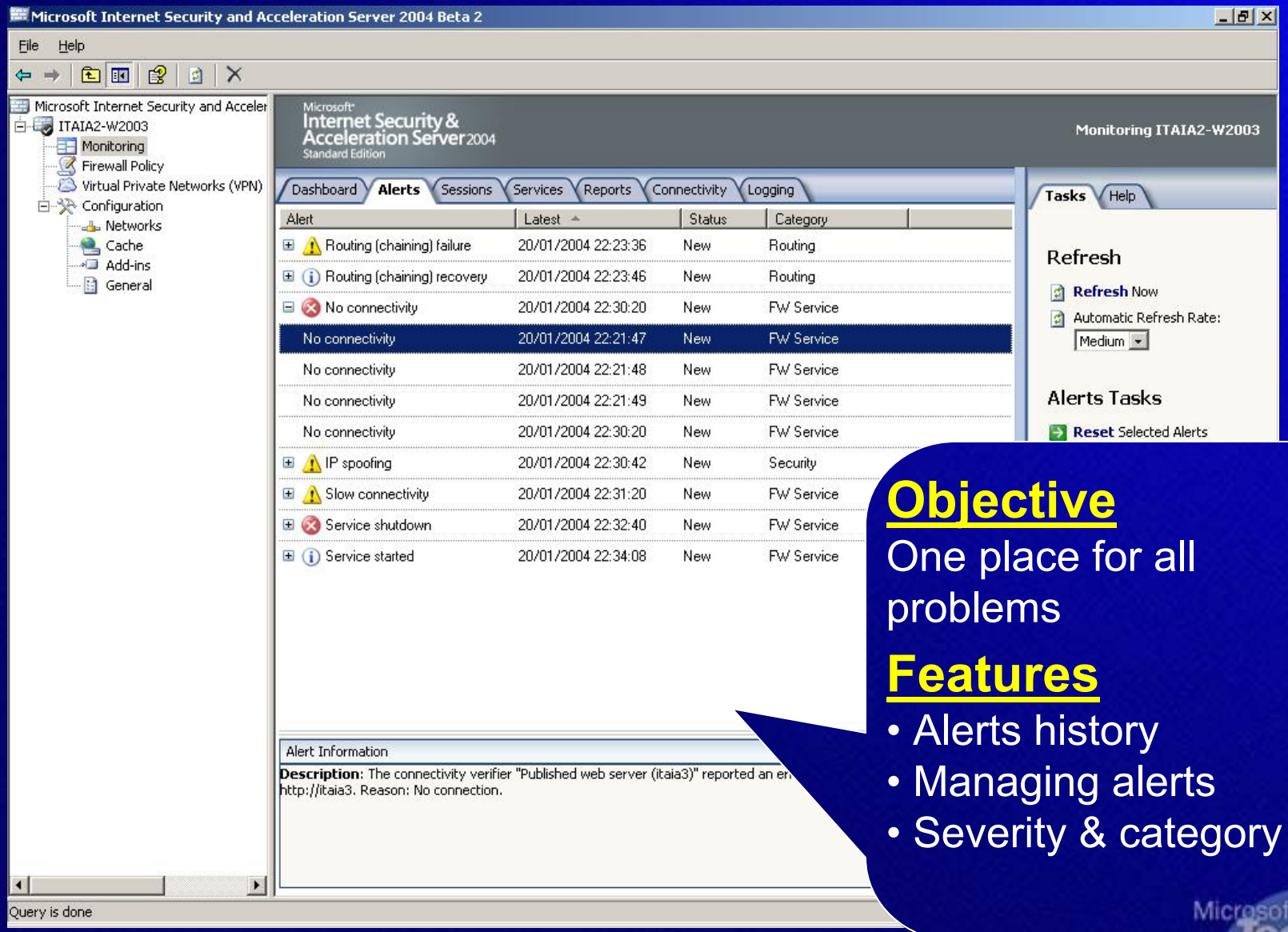
Objective

Centralized status view

Features

- Real time
- Aggregated
- Easy to spot problems

Alerts


Microsoft Internet Security and Acceleration Server 2004 Beta 2
File Help
Microsoft Internet Security and Acceler
ITAIA2-W2003
Monitoring
Firewall Policy
Virtual Private Networks (VPN)
Configuration
Networks
Cache
Add-ins
General
Microsoft Internet Security & Acceleration Server 2004
Standard Edition
Monitoring ITAIA2-W2003
Dashboard Alerts Sessions Services Reports Connectivity Logging
Alert Latest Status Category
Routing (chaining) failure 20/01/2004 22:23:36 New Routing
Routing (chaining) recovery 20/01/2004 22:23:46 New Routing
No connectivity 20/01/2004 22:30:20 New FW Service
No connectivity 20/01/2004 22:21:47 New FW Service
No connectivity 20/01/2004 22:21:48 New FW Service
No connectivity 20/01/2004 22:21:49 New FW Service
No connectivity 20/01/2004 22:30:20 New FW Service
IP spoofing 20/01/2004 22:30:42 New Security
Slow connectivity 20/01/2004 22:31:20 New FW Service
Service shutdown 20/01/2004 22:32:40 New FW Service
Service started 20/01/2004 22:34:08 New FW Service
Tasks Help
Refresh
Refresh Now
Automatic Refresh Rate:
Medium
Alerts Tasks
Reset Selected Alerts
Alert Information
Description: The connectivity verifier "Published web server (itaia3)" reported an er
http://itaia3. Reason: No connection.
Query is done

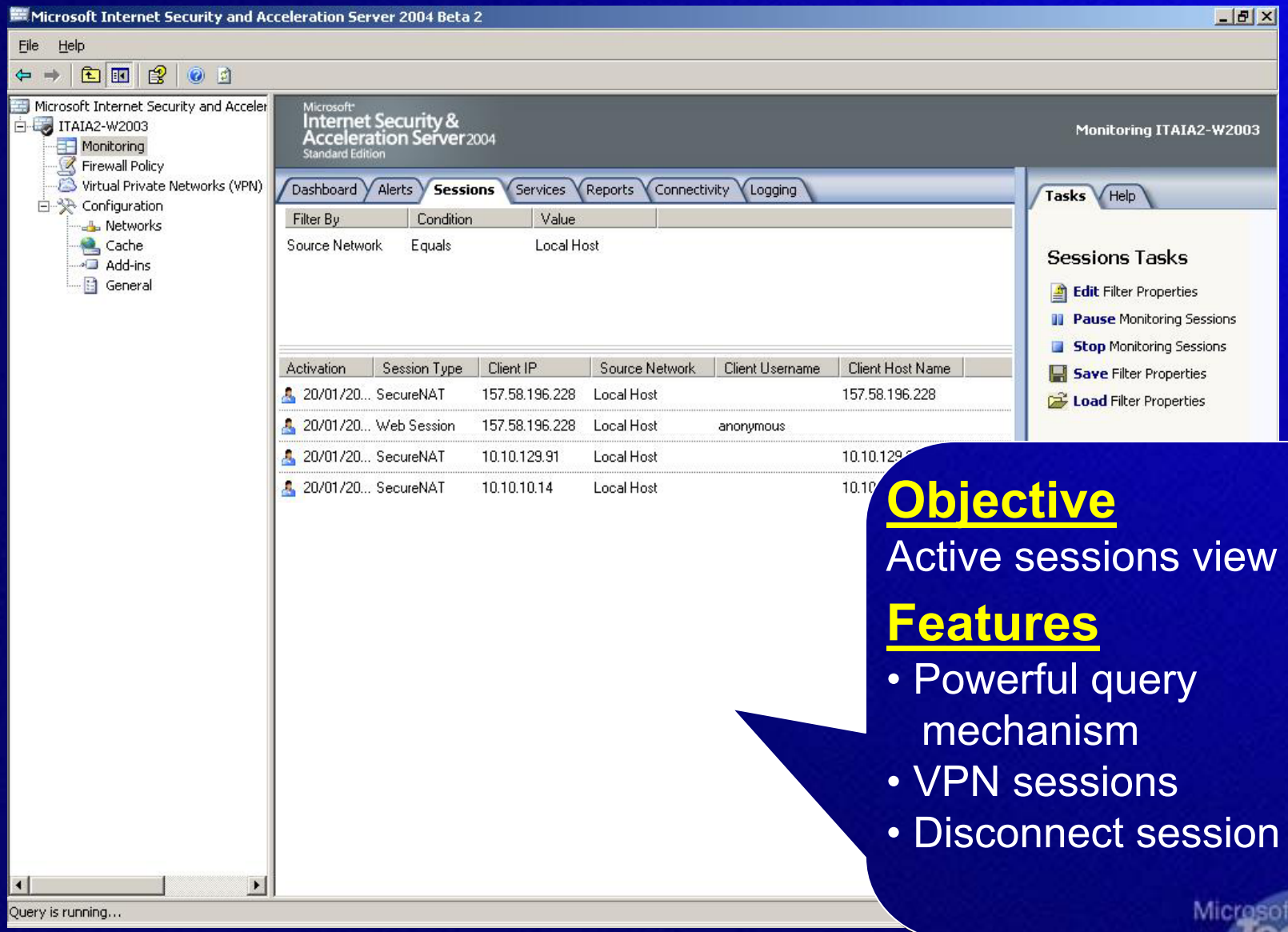
Objective

One place for all problems

Features

- Alerts history
- Managing alerts
- Severity & category

Sessions



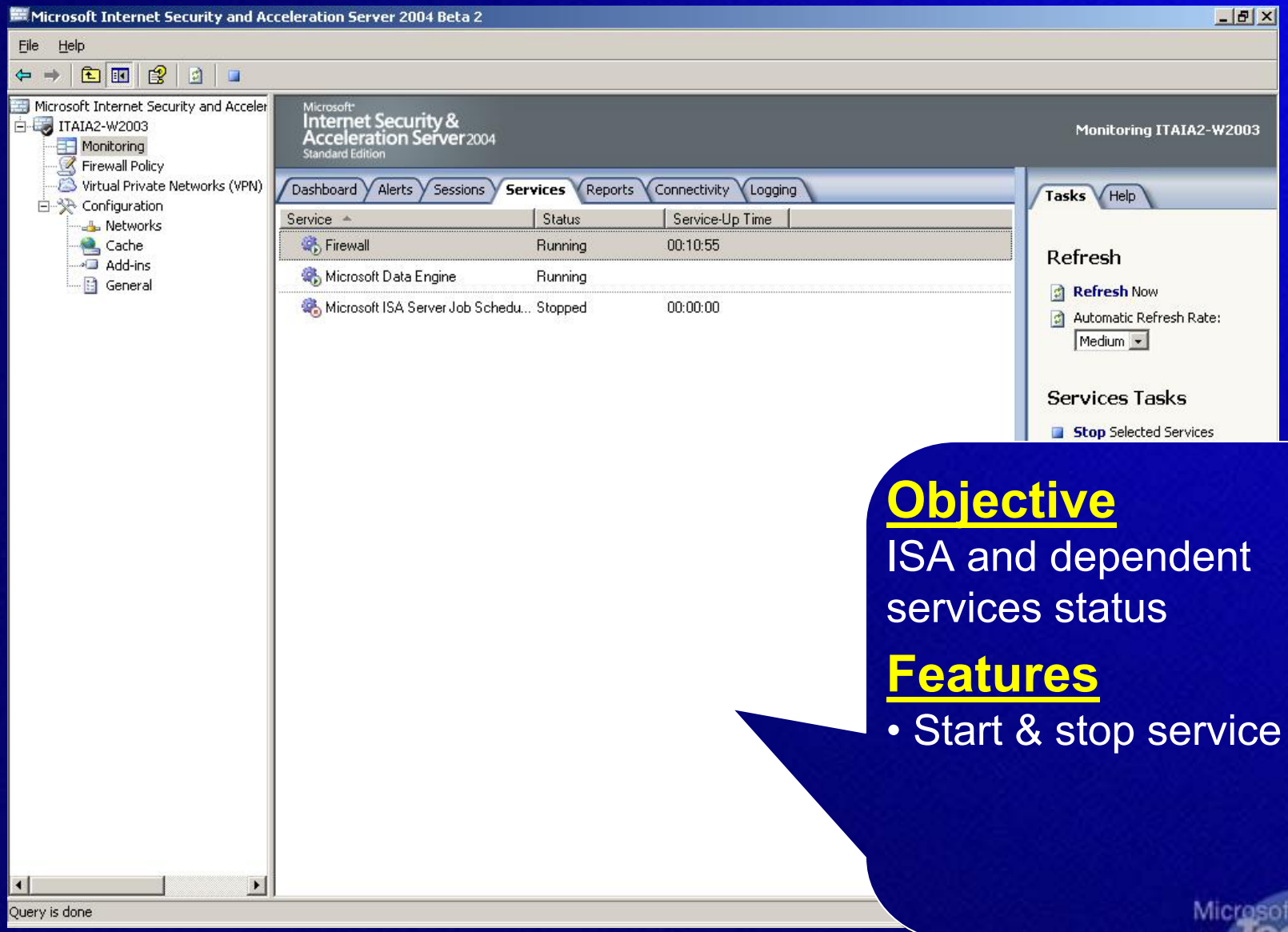
Objective

Active sessions view

Features

- Powerful query mechanism
- VPN sessions
- Disconnect session

Services



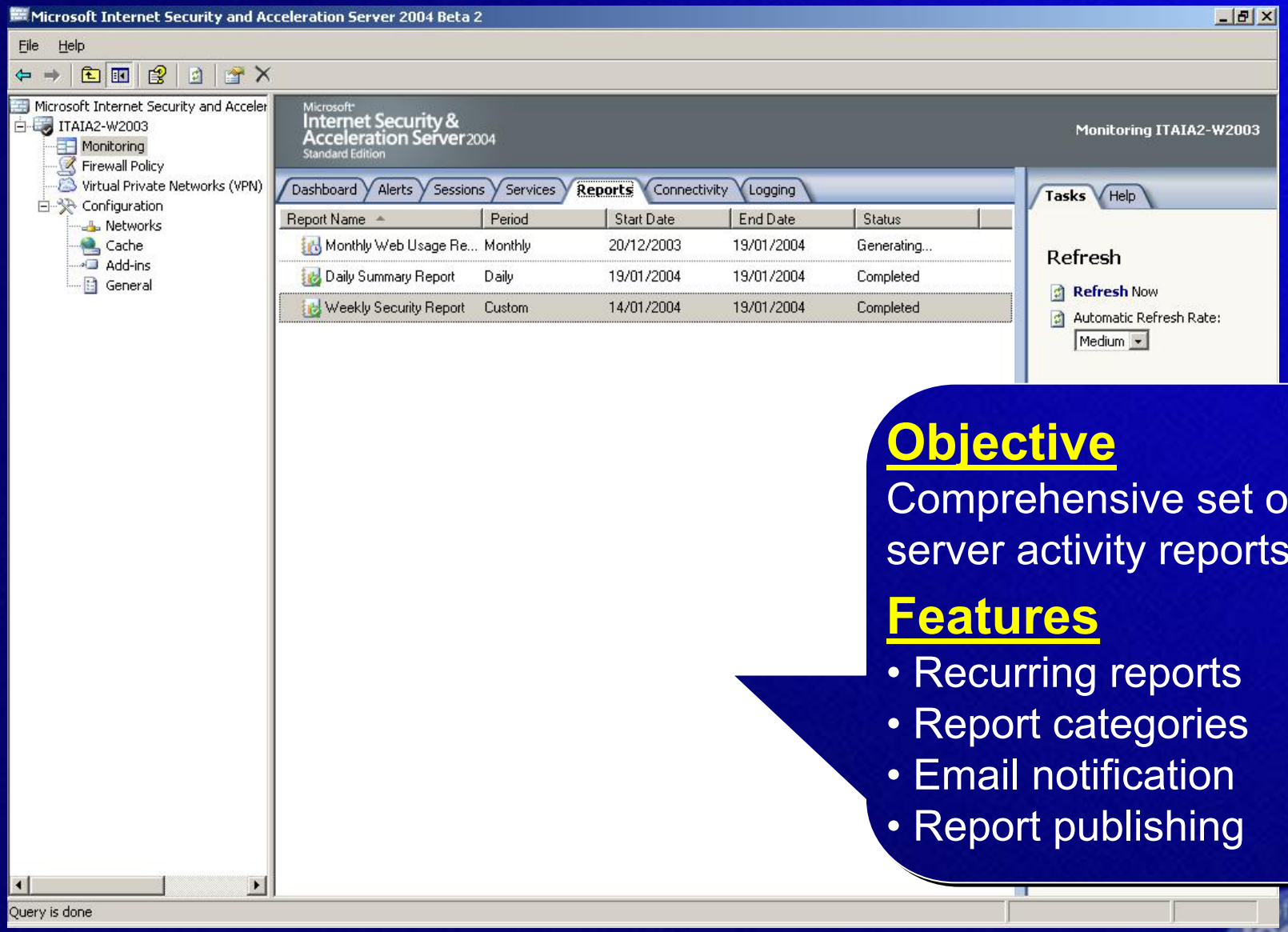
Objective

ISA and dependent services status

Features

- Start & stop service

Reports



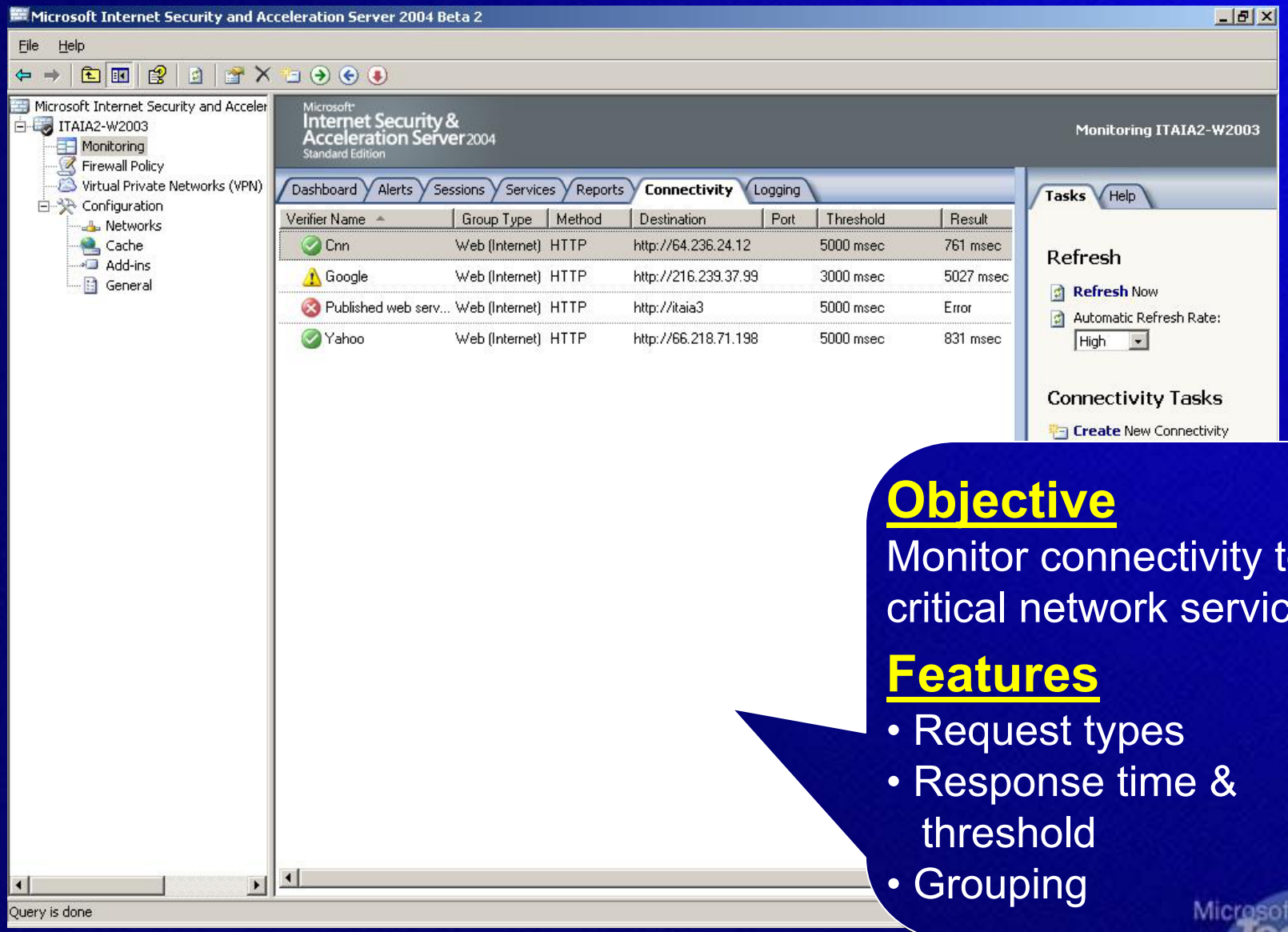
Objective

Comprehensive set of server activity reports

Features

- Recurring reports
- Report categories
- Email notification
- Report publishing

Connectivity



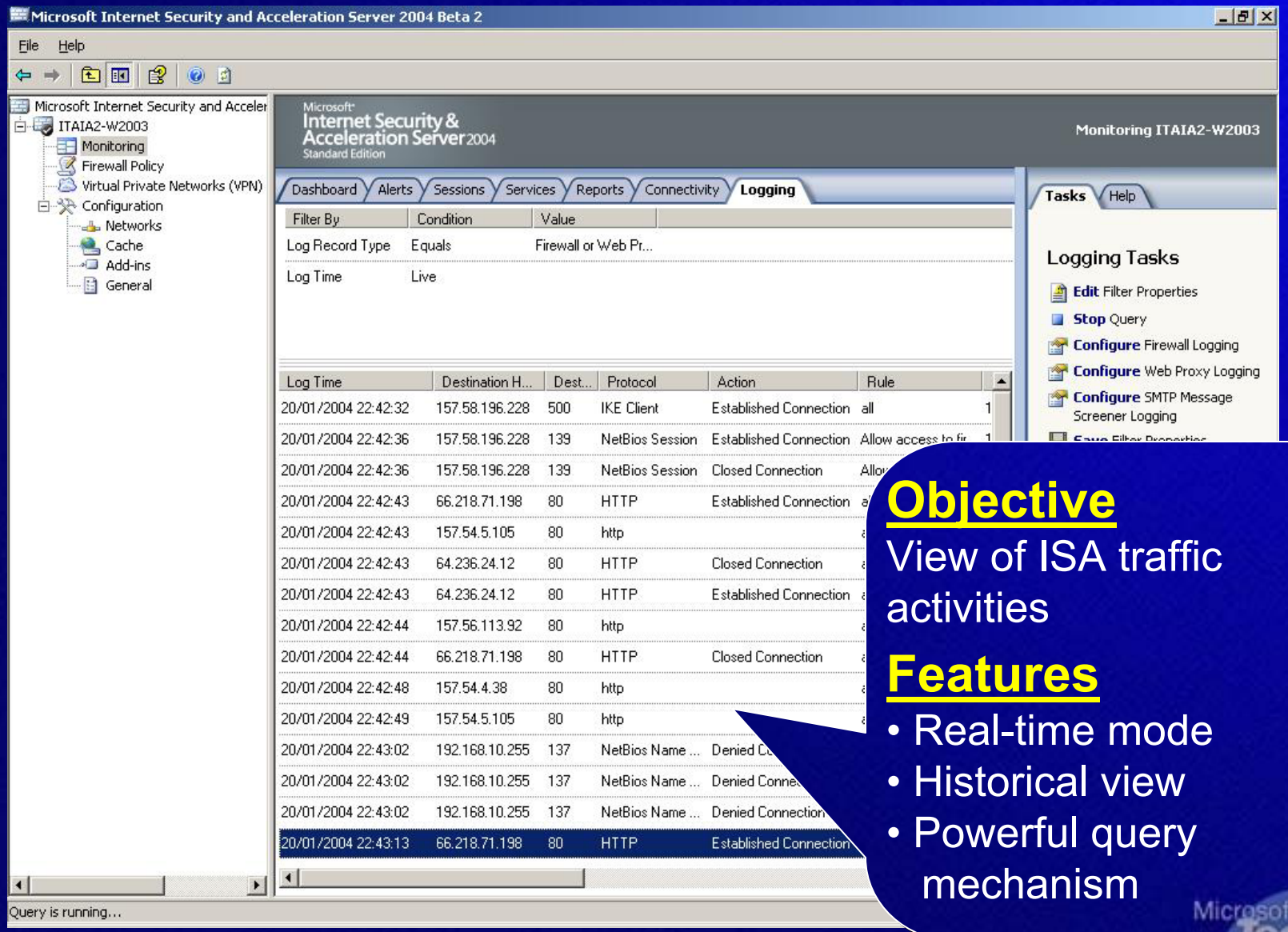
Objective

Monitor connectivity to critical network services

Features

- Request types
- Response time & threshold
- Grouping

Logging


Microsoft Internet Security and Acceleration Server 2004 Beta 2
File Help
Microsoft Internet Security and Acceler
ITAIA2-W2003
Monitoring
Firewall Policy
Virtual Private Networks (VPN)
Configuration
Networks
Cache
Add-ins
General
Microsoft Internet Security & Acceleration Server 2004 Standard Edition
Monitoring ITAIA2-W2003
Dashboard Alerts Sessions Services Reports Connectivity Logging
Filter By Condition Value
Log Record Type Equals Firewall or Web Pr...
Log Time Live
Log Time Destination H... Dest... Protocol Action Rule
20/01/2004 22:42:32 157.58.196.228 500 IKE Client Established Connection all
20/01/2004 22:42:36 157.58.196.228 139 NetBios Session Established Connection
20/01/2004 22:42:36 157.58.196.228 139 NetBios Session Closed Connection
20/01/2004 22:42:43 66.218.71.198 80 HTTP Established Connection
20/01/2004 22:42:43 157.54.5.105 80 http
20/01/2004 22:42:43 64.236.24.12 80 HTTP Closed Connection
20/01/2004 22:42:43 64.236.24.12 80 HTTP Established Connection
20/01/2004 22:42:44 157.56.113.92 80 http
20/01/2004 22:42:44 66.218.71.198 80 HTTP Closed Connection
20/01/2004 22:42:48 157.54.4.38 80 http
20/01/2004 22:42:49 157.54.5.105 80 http
20/01/2004 22:43:02 192.168.10.255 137 NetBios Name ... Denied
20/01/2004 22:43:02 192.168.10.255 137 NetBios Name ... Denied
20/01/2004 22:43:02 192.168.10.255 137 NetBios Name ... Denied Connection
20/01/2004 22:43:13 66.218.71.198 80 HTTP Established Connection
Tasks Help
Logging Tasks
Edit Filter Properties
Stop Query
Configure Firewall Logging
Configure Web Proxy Logging
Configure SMTP Message Screener Logging
Query is running...

Objective

View of ISA traffic activities

Features

- Real-time mode
- Historical view
- Powerful query mechanism

Performance

Enhanced Architecture

- **Optimized for real life usage scenarios**
- **Improvements since ISA Server 2000**
  - **Kernel-mode data pump**
  - **User-mode optimizations**
  - **Up to +150% (2.5X faster) for firewall (SecureNAT) traffic**
  - **Up to +250% (3.5X faster) for Web (transparent) proxy traffic**
  - **1,000,000+ concurrent connections**
- **Scale up with additional CPUs**

Raw throughput performance

Test	Results	Details
KM tput, 1500 MTU	1.65 Gbps	2-proc, 4 NICs
KM tput, 9000 MTU	4.6 Gbps	4-proc, 6 NICs
HTTP Filtering	250 Mbps @ 600 cps	2-proc, 4 NICs

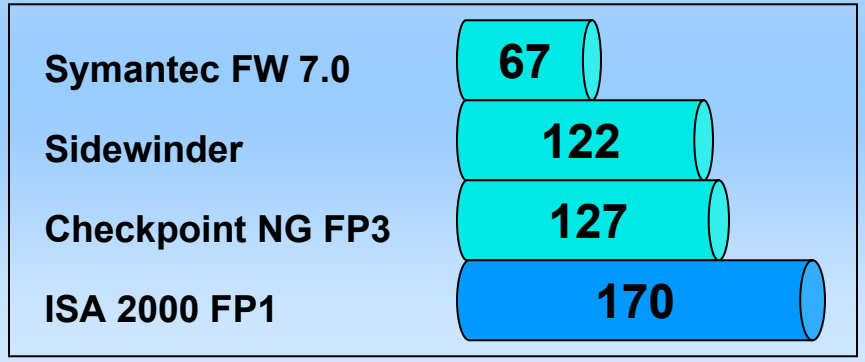
How?

- **Design improvements**
- **IP Stack improvements**
- **Hardware improvements**

(raw thru-put measured using HTTP+NAT benchmark)

Network Computing Magazine app. layer firewall review (3/03):

Full inspection performance [Mbps]



Updated Firewall Client

- What is the ISA Firewall Client?
  - Enables / disables Winsock application connectivity to the Internet
  - Provides network access across ISA for Winsock-compatible applications.
    - Makes intelligent decisions about the destination of traffic based on destination address
    - Will automatically detect the available firewall on the network
- What is new in ISA Firewall Client 2004?
  - Uses a secure encrypted channel with ISA Server 2004
  - Supports multiple users' settings preferences
    - Allows two profile users to configure the firewall client to use different proxy servers

Microsoft TechNet

Migration Planning

- ISA 2000 SE > ISA 2004 SE
  - Policy migration tool
  - Recommend fresh approach
- ISA 2000 EE > ISA 2004 EE
  - Configuration migration capabiltiy
- ISA 2004 EE Beta > ISA 2004 EE RTM
  - Upgrade capability to be confirmed
- ISA 2004 SE > ISA 2004 EE
  - Policy extraction tool to be confirmed

Subject to change